

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Masashi MORIOKA, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: METHOD OF AUTHENTICATION AND PAYMENT, OPERATION METHOD OF AN AUTHENTICATION AND PAYMENT SYSTEM, TERMINAL DEVICE, SERVICE PROVIDING DEVICE, AUTHENTICATION AND PAYMENT DEVICE, AND CONTROL INFORMATION PROVIDING DEVICE

**REQUEST FOR PRIORITY**

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number \_\_\_\_\_, filed \_\_\_\_\_, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):  
**Application No.** **Date Filed**

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

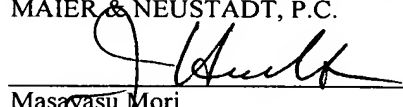
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-289191	October 1, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. \_\_\_\_\_ filed \_\_\_\_\_
- ☐ were submitted to the International Bureau in PCT Application Number \_\_\_\_\_  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. \_\_\_\_\_ filed \_\_\_\_\_; and
- ☐ (B) Application Serial No.(s)  
☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

  
Masayasu Mori

Registration No. 47,301

James D. Hamilton  
Registration No. 28,421

Customer Number

**22850**

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 2 年 1 0 月 1 日

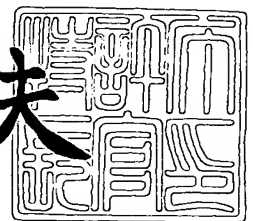
出 願 番 号  
Application Number: 特 願 2 0 0 2 - 2 8 9 1 9 1  
[ST. 10/C]: [ J P 2 0 0 2 - 2 8 9 1 9 1 ]

出 願 人  
Applicant(s): 株式会社エヌ・ティ・ティ・ドコモ

2 0 0 3 年 9 月 1 1 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 7 4 9 4 8

【書類名】 特許願

【整理番号】 DCMH140388

【提出日】 平成14年10月 1日

【あて先】 特許庁長官殿

【国際特許分類】 H04Q 7/00

【発明の名称】 認証決済方法、端末装置、サービス提供装置、認証決済装置、制御情報提供装置及び認証決済システム

【請求項の数】 23

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社 エヌ・ティ・ティ・ドコモ内

【氏名】 森岡 将史

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社 エヌ・ティ・ティ・ドコモ内

【氏名】 栄藤 稔

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社 エヌ・ティ・ティ・ドコモ内

【氏名】 米本 佳史

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社 エヌ・ティ・ティ・ドコモ内

【氏名】 鈴木 敬

【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社 エヌ・ティ・ティ・ドコモ

## 【代理人】

【識別番号】 100083806

【弁理士】

【氏名又は名称】 三好 秀和

【電話番号】 03-3504-3075

## 【選任した代理人】

【識別番号】 100100712

【弁理士】

【氏名又は名称】 岩▲崎▼ 幸邦

## 【選任した代理人】

【識別番号】 100095500

【弁理士】

【氏名又は名称】 伊藤 正和

## 【選任した代理人】

【識別番号】 100101247

【弁理士】

【氏名又は名称】 高橋 俊一

## 【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9702416

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証決済方法、端末装置、サービス提供装置、認証決済装置、制御情報提供装置及び認証決済システム

【特許請求の範囲】

【請求項 1】 端末装置、1 又は複数のサーバ、これらを結ぶネットワークから構成される認証決済システムにおける認証決済方法であって、

前記 1 又は複数のサーバが、前記端末装置からのネットワークを介したサービス利用要求に対して、当該端末装置の送信するサービス証明書記載内容、ネットワーク環境、システム運用ポリシーのうちの少なくとも 1 つの状況に適応して、サービス手順及び／又はメッセージフォーマットを切換えて当該認証決済システムを運用することを特徴とする認証決済方法。

【請求項 2】 認証決済装置からネットワークを通じて所定情報の組み込まれた第 1 の電子サービス証明書を受信する手段と、

前記第 1 の電子サービス証明書を加工し、当該端末装置を識別する情報を含む第 2 の電子サービス証明書を生成し、サービス提供装置にネットワークを通じて送信する手段とを備えたことを特徴とする端末装置。

【請求項 3】 前記第 1 の電子サービス証明書の全部又は一部をそのまま第 2 の電子サービス証明書とし、前記第 1 の電子サービス証明書の全部又は一部に新たな情報を付加して第 2 の電子サービス証明書とし、前記第 1 の電子サービス証明書の全部又は一部に電子署名を付加して第 2 の電子サービス証明書とし、又は、前記第 1 の電子サービス証明書の全部又は一部に新たな情報と電子署名を付加して第 2 の電子サービス証明書とすることを特徴とする請求項 2 に記載の端末装置。

【請求項 4】 前記第 1 の電子サービス証明書から抽出したサービス証明書識別子、認証決済装置識別子又は認証決済装置の電子署名のうちの少なくとも 1 つを含む識別情報又はこれに新たに情報を付加した情報をそのまま第 2 の電子サービス証明書とし、又は前記情報に電子署名を付加して第 2 の電子サービス証明書とすることを特徴とする請求項 3 に記載の端末装置。

【請求項 5】 認証決済装置からネットワークを通じて配布された電子サー

ビス証明書の利用履歴を管理する手段と、

当該利用履歴が当該電子サービス証明書に記載された条件を満たしたときに前記認証決済装置に通知する手段とを備えたことを特徴とする端末装置。

【請求項 6】 端末装置からネットワークを通じて電子サービス証明書を受信する手段と、

認証決済装置に認証決済要求をネットワークを通じて送信する手段とを備えたことを特徴とするサービス提供装置。

【請求項 7】 前記電子サービス証明書の全部又は一部をそのまま用い、又はこれに新たに情報を付加して認証決済要求を生成し、当該認証決済要求をそのまま又はこれに電子署名を付加して送信することを特徴とする請求項 6 に記載のサービス提供装置。

【請求項 8】 前記電子サービス証明書から抽出したサービス証明書識別子、認証決済装置識別子又は認証決済装置の電子署名のうち少なくとも 1 つを含む識別情報をそのまま用い、又はこれに新たに情報を付加して認証決済要求を生成し、当該認証決済要求をそのまま又はこれに電子署名を付加して送信することを特徴とする請求項 7 に記載のサービス提供装置。

【請求項 9】 端末装置のサービス要求に対応したサービス提供を行う時点と認証決済装置に対する認証決済要求処理を行う時点との使い分け、又は認証決済要求処理の簡略化を行う制御手段を備えたことを特徴とする請求項 6 に記載のサービス提供装置。

【請求項 1 0】 端末装置からネットワークを通じて第 1 の電子サービス証明書を受信する手段と、

前記第 1 の電子サービス証明書に所定の情報を付加して第 2 の電子サービス証明書を生成し、前記端末装置にネットワークを通じて送信する手段とを備えたことを特徴とする請求項 6 に記載のサービス提供装置。

【請求項 1 1】 他の装置に対する電子サービス証明書を発行する手段と、

他の装置からネットワークを通じて受信した認証決済要求の正当性の検証、前記認証決済要求の認証、前記認証決済要求が対象とするサービス提供の許可、当該サービス提供に対する決済の少なくとも 1 つの処理を行う手段とを備えたこと

を特徴とする認証決済装置。

【請求項 12】 前記電子サービス証明書に、当該サービス証明書識別子と、当該認証決済装置識別子と、前記他の装置の識別子と、当該サービス証明書有効期間と前記他の装置に対するサービス制約条件のうち少なくとも 1 つの情報を含めることを特徴とする請求項 11 に記載の認証決済装置。

【請求項 13】 前記電子サービス証明書に本来的に含めるべき情報の全部又は一部を蓄積情報として蓄積する情報蓄積手段を備え、

前記電子サービス証明書には、前記情報蓄積手段における前記蓄積情報の蓄積位置を示す情報を含めることを特徴とする請求項 11 に記載の認証決済装置。

【請求項 14】 前記電子サービス証明書を、他の装置の要求に応じて又は予め設定されている送信条件に該当するときに自発的に当該他の装置に送信することを特徴とする請求項 11 に記載の認証決済装置。

【請求項 15】 管理下にある情報の更新を契機に前記電子サービス証明書の内容を更新し、該当する他の装置に送信することを特徴とする請求項 14 に記載の認証決済装置。

【請求項 16】 前記電子サービス証明書を定期的に更新することを特徴とする請求項 14 に記載の認証決済装置。

【請求項 17】 端末装置、サービス提供装置、認証決済装置及びこれらを結ぶネットワークから構成される認証決済システムであって、

前記端末装置からのネットワークを介したサービス利用要求に対して、当該端末装置の送信するサービス証明書記載内容、ネットワーク環境、システム運用ポリシーのうちの少なくとも 1 つの状況に適応して、サービス手順及び／又はメッセージフォーマットを切換えて当該システムを運用することを特徴とする認証決済システム。

【請求項 18】 サービス証明書記載内容、ネットワーク環境、システム運用ポリシーのうちの少なくとも 1 つの状況に適応する制御情報を生成し及び／又はネットワーク上に公開することを特徴とする制御情報提供装置。

【請求項 19】 前記制御情報の記述に識別子を付加した情報を生成し及び／又は公開することを特徴とする請求項 18 に記載の制御情報提供装置。

【請求項 20】 前記制御情報の記述は、これを利用する装置の能力に合わせて修正することを特徴とする請求項 19 記載の制御情報提供装置。

【請求項 21】 前記制御情報に従った動作を実現するソフトウェアを生成し及び／又は公開する請求項 18 に記載の制御情報提供装置。

【請求項 22】 動的にソフトウェアを生成し、当該ソフトウェアのキャッシュを行うことを特徴とする請求項 21 に記載の制御情報提供装置。

【請求項 23】 当該ソフトウェアを動作させる装置能力に合わせてソフトウェアを生成し及び／又は公開することを特徴とする請求項 21 に記載の制御情報提供装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、ネットワークを介した認証決済システムとシステムの構成装置に関する。

【0002】

【従来の技術】

インターネットや携帯電話機を決済手段として活用した飲料や書籍の購入、音楽・映像などのコンテンツ配信、ネットワークサービス利用などの電子商取引が普及してきており、これにより手元に金銭を用意することなくサービスや商品の購入・利用が可能となっている。このような取引を行うための従来の手順の例として特許文献 1 や非特許文献 1 に記載されたものがある。これらの従来例では取引を行う度に決済を行う手段が述べられている。

【0003】

ところが、このように定められた決済方法では、商品やサービスの提供における要求条件に合致しない場合がある。例えば戸外において携帯電話機を用いて飲料を購入する場合、短時間に購入したいという利用者の要求があるにも拘らず、サービス要求からサービス提供までに数秒から数十秒程度の時間が必要となり、顧客を待たせてしまうという問題点がある。

【0004】



このような問題点を解決するため、非特許文献 2 では、ポリシーや金額に応じて商品提供を決済に先行して行う方式が記載されている。この場合、決済者は取引毎に決済を行うのではなく、複数の決済処理を一括して行うことが記述されている。

#### 【 0 0 0 5 】

しかしながら、このようにサービス利用と決済処理との間にタイムラグがあると、1 回 1 回の利用金額は小さくても利用回数が多くなると合計の利用金額が高額になってしまう可能性があり、その場合には、Provisional Agent と呼ばれる装置がリスクを負ってしまう問題点がある。

#### 【 0 0 0 6 】

他方、このようなポリシーに応じて商品提供を決済に先行させるだけでなく、ポリシーを含めた様々な要求条件に適合可能なシステムの従来例として、メッセージフローやメッセージフォーマットの適応的な変更を可能にする技術が特許文献 2 に記載されている。この従来例は、サービス・サーバのサービス仕様を定めるステップを定め、当該サービス仕様に従って各エンティティを動作させることによって、サービス提供方法に柔軟性を持つシステムを実現し、通信履歴情報を含むクーポンを用いてサービスを行うか否かを判定する技術である。

#### 【 0 0 0 7 】

##### 【特許文献 1】

特開 2 0 0 1 - 1 4 8 0 4 8 号公報

#### 【 0 0 0 8 】

##### 【特許文献 2】

特許第 3 2 2 4 7 8 4 号公報

#### 【 0 0 0 9 】

##### 【非特許文献 1】

"MeT WAP Shopping",

(<http://www.mobiletransaction.org/pdf/R11/MeT-WAP-Shopping-R11.pdf>)

#### 【 0 0 1 0 】

##### 【非特許文献 2】

Matt Blaze, John Ioannidis, and Angelos D. Keromytis,  
"Offline Micropayments without Trusted Hardware",  
(<http://www.crypto.com/papers/knpay.pdf>)

【 0 0 1 1 】

【発明が解決しようとする課題】

本発明は、上述した従来の技術的課題に鑑みてなされたもので、ネットワーク上での認証や決済が必要となる手順において、利用者の許容待ち時間、ネットワーク環境や運用ポリシーといった状況に応じてリスク管理が行える技術を提供することを目的とする。

【 0 0 1 2 】

【課題を解決するための手段】

請求項 1 の発明は、端末装置、1 又は複数のサーバ、これらを結ぶネットワークから構成される認証決済システムにおける認証決済方法であって、前記 1 又は複数のサーバが、前記端末装置からのネットワークを介したサービス利用要求に対して、当該端末装置の送信するサービス証明書記載内容、ネットワーク環境、システム運用ポリシーのうちの少なくとも 1 つの状況に適応して、サービス手順及び／又はメッセージフォーマットを切換えて当該認証決済システムを運用することを特徴とするものである。

【 0 0 1 3 】

請求項 2 の発明の端末装置は、認証決済装置からネットワークを通じて所定情報の組み込まれた第 1 の電子サービス証明書を受信する手段と、前記第 1 の電子サービス証明書を加工し、当該端末装置を識別する情報を含む第 2 の電子サービス証明書を生成し、サービス提供装置にネットワークを通じて送信する手段とを備えたものである。

【 0 0 1 4 】

請求項 3 の発明は、請求項 2 の端末装置において、前記第 1 の電子サービス証明書の全部又は一部をそのまま第 2 の電子サービス証明書とし、前記第 1 の電子サービス証明書の全部又は一部に新たな情報を付加して第 2 の電子サービス証明書とし、前記第 1 の電子サービス証明書の全部又は一部に電子署名を付加して第

2の電子サービス証明書とし、又は、前記第1の電子サービス証明書の全部又は一部に新たな情報と電子署名を付加して第2の電子サービス証明書とすることを特徴とするものである。

【0015】

請求項4の発明は、請求項3の端末装置において、前記第1の電子サービス証明書から抽出したサービス証明書識別子、認証決済装置識別子又は認証決済装置の電子署名のうちの少なくとも1つを含む識別情報又はこれに新たに情報を付加した情報をそのまま第2の電子サービス証明書とし、又は前記情報に電子署名を付加して第2の電子サービス証明書とすることを特徴とするものである。

【0016】

請求項5の発明の端末装置は、認証決済装置からネットワークを通じて配布された電子サービス証明書の利用履歴を管理する手段と、当該利用履歴が当該電子サービス証明書に記載された条件を満たしたときに前記認証決済装置に通知する手段とを備えたものである。

【0017】

請求項6の発明のサービス提供装置は、端末装置からネットワークを通じて電子サービス証明書を受信する手段と、認証決済装置に認証決済要求をネットワークを通じて送信する手段とを備えたものである。

【0018】

請求項7の発明は、請求項6のサービス提供装置において、前記電子サービス証明書の全部又は一部をそのまま用い、又はこれに新たに情報を付加して認証決済要求を生成し、当該認証決済要求をそのまま又はこれに電子署名を付加して送信することを特徴とするものである。

【0019】

請求項8の発明は、請求項7のサービス提供装置において、前記電子サービス証明書から抽出したサービス証明書識別子、認証決済装置識別子又は認証決済装置の電子署名のうち少なくとも1つを含む識別情報をそのまま用い、又はこれに新たに情報を付加して認証決済要求を生成し、当該認証決済要求をそのまま又はこれに電子署名を付加して送信することを特徴とするものである。

**【0020】**

請求項9の発明は、請求項6のサービス提供装置において、端末装置のサービス要求に対応したサービス提供を行う時点と認証決済装置に対する認証決済要求処理を行う時点との使い分け、又は認証決済要求処理の簡略化を行う制御手段を備えたことを特徴とするものである。

**【0021】**

請求項10の発明は、請求項6のサービス提供装置において、端末装置からネットワークを通じて第1の電子サービス証明書を受信する手段と、前記第1の電子サービス証明書に所定の情報を付加して第2の電子サービス証明書を生成し、前記端末装置にネットワークを通じて送信する手段とを備えたことを特徴とするものである。

**【0022】**

請求項11の発明の認証決済装置は、他の装置に対する電子サービス証明書を発行する手段と、他の装置からネットワークを通じて受信した認証決済要求の正当性の検証、前記認証決済要求の認証、前記認証決済要求が対象とするサービス提供の許可、当該サービス提供に対する決済の少なくとも1つの処理を行う手段とを備えたものである。

**【0023】**

請求項12の発明は、請求項11の認証決済装置において、前記電子サービス証明書に、当該サービス証明書識別子と、当該認証決済装置識別子と、前記他の装置の識別子と、当該サービス証明書有効期間と前記他の装置に対するサービス制約条件のうち少なくとも1つの情報を含めることを特徴とするものである。

**【0024】**

請求項13の発明は、請求項11の認証決済装置において、前記電子サービス証明書に本来的に含めるべき情報の全部又は一部を蓄積情報として蓄積する情報蓄積手段を備え、前記電子サービス証明書には、前記情報蓄積手段における前記蓄積情報の蓄積位置を示す情報を含めることを特徴とするものである。

**【0025】**

請求項14の発明は、請求項11の認証決済装置において、前記電子サービス

証明書を、他の装置の要求に応じて又は予め設定されている送信条件に該当するときに自発的に当該他の装置に送信することを特徴とするものである。

【0026】

請求項15の発明は、請求項14の認証決済装置において、管理下にある情報の更新を契機に前記電子サービス証明書の内容を更新し、該当する他の装置に送信することを特徴とするものである。

【0027】

請求項16の発明は、請求項14の認証決済装置において、前記電子サービス証明書を定期的に更新することを特徴とするものである。

【0028】

請求項17の発明は、端末装置、サービス提供装置、認証決済装置及びこれらを結ぶネットワークから構成される認証決済システムであって、前記端末装置からのネットワークを介したサービス利用要求に対して、当該端末装置の送信するサービス証明書記載内容、ネットワーク環境、システム運用ポリシーのうちの少なくとも1つの状況に適応して、サービス手順及び／又はメッセージフォーマットを切換えて当該システムを運用するものである。

【0029】

請求項18の発明の制御情報提供装置は、サービス証明書記載内容、ネットワーク環境、システム運用ポリシーのうちの少なくとも1つの状況に適応する制御情報を生成し及び／又はネットワーク上に公開するものである。

【0030】

請求項19の発明は、請求項18の制御情報提供装置において、前記制御情報の記述に識別子を付加した情報を生成し及び／又は公開することを特徴とするものである。

【0031】

請求項20の発明は、請求項19の制御情報提供装置において、前記制御情報の記述は、これを利用する装置の能力に合わせて修正することを特徴とするものである。

【0032】

請求項 21 の発明は、請求項 18 の制御情報提供装置において、前記制御情報に従った動作を実現するソフトウェアを生成し及び／又は公開することを特徴とするものである。

#### 【0033】

請求項 22 の発明は、請求項 21 の制御情報提供装置において、動的にソフトウェアを生成し、当該ソフトウェアのキャッシュを行うことを特徴とするものである。

#### 【0034】

請求項 23 の発明は、請求項 21 の制御情報提供装置において、当該ソフトウェアを動作させる装置能力に合わせてソフトウェアを生成し及び／又は公開することを特徴とするものである。

#### 【0035】

本発明では、サービス証明書に記載された顧客の利用可能金額、通信路のセキュリティ強度、伝送帯域、位置などのネットワーク環境や運用ポリシーなどの状況に適応して暗号化、署名の付加などサービス手順及び／又はメッセージフォーマットを適応的に使い分けることにより、サービス提供時間の短縮化、セキュリティ強度の調節、伝送情報の削減等を行うことが可能である。

#### 【0036】

この場合、すべての情報を暗号化し、あるいはすべての情報に署名を付与するのではなく、一部分を暗号化しあるいは一部分に署名を付与するようにすれば、重要部分のみ暗号化することが可能になる。

#### 【0037】

また、これらのメッセージの一部をメッセージ本文に含めるのではなくて蓄積装置に蓄積し、メッセージ本文には当該蓄積装置での蓄積位置の参照情報を含めるようにすれば、伝送情報の量を削減することができる。これは利用率が低い情報の添付に特に有効である。

#### 【0038】

本発明ではまた、端末装置及びサービス提供装置から信頼された認証決済装置が端末装置に対し、サービス提供装置が認証、サービス許可、決済を行う上での

信用情報、補助情報を含むサービス証明書を署名付きで発行し、端末装置が認証決済装置の発行した当該署名付きサービス証明書に情報を付加してサービス提供装置に送信するようにすることにより、認証決済装置が顧客を保証し、サービス提供装置はサービス証明書の署名検証による正当性を確認するのみで、リスクが小さな場合には、複雑な認証、サービス許可や決済処理に先行してサービス提供を行うことが可能である。

#### 【 0 0 3 9 】

この場合、サービス証明書を転送する際に必須情報のみ抽出して送信するようにすれば、伝送情報の削減が可能になる。

#### 【 0 0 4 0 】

また、サービス提供装置が端末装置から受信したサービス証明書に情報を付加して認証決済装置に送信するようにすれば、認証決済装置において顧客情報の更新、決済処理を行い、サービス証明書の内容更新に繋げることができる。

#### 【 0 0 4 1 】

またさらに、認証決済装置における顧客情報の更新を契機にサービス証明書を端末装置に送信したり、定期的にサービス証明書を更新するようにしたりすれば、端末装置は常に最新の情報を反映したサービス証明書を保持でき、サービス提供装置のリスクを減少させることができる。

#### 【 0 0 4 2 】

また本発明では、端末装置が、状況に適應する制御情報を生成し公開する制御情報提供装置からサービスフローやメッセージフォーマットのようなサービスインタフェースを取得し、それに従って動作することにより、状況に適應して柔軟なサービス要求を行うことが可能である。

#### 【 0 0 4 3 】

この場合、当該サービスインタフェースの記述に一意的な識別子を付与するようにすれば、当該識別子によりサービスインタフェースを同定できるようになり、同一のインタフェースを用いるサービスを利用する場合に、再度当該サービスインタフェースをダウンロードする回数を減少させることが可能になる。

#### 【 0 0 4 4 】

また、当該制御情報提供装置が当該サービスインタフェースに電子署名を行うようにすれば、当該サービスインタフェースの否認防止、完全性保証を行うことが可能になる。

#### 【0 0 4 5】

また、当該サービスインタフェース情報をもとに端末装置で動作するソフトウェアを生成し、端末装置上で動作させるようにすれば、端末装置が必ずしも当該サービスインタフェース記述を理解して動作する必要性がなくなり、また、端末装置の機能に合わせたソフトウェアを生成するようにすれば、当該ソフトウェアのサイズを減少させることが可能になり、伝送情報量、端末装置における記憶領域の使用量を削減することができる。

#### 【0 0 4 6】

さらにまた、制御情報提供装置において生成したソフトウェアをキャッシュし、同一のソフトウェアを要求された場合に当該キャッシュから読み出して送信を行うようにすれば、当該ソフトウェアの生成コスト、時間の短縮が可能になる。

#### 【0 0 4 7】

##### 【発明の実施の形態】

以下、本発明の実施の形態を図に基づいて詳説する。

#### 【0 0 4 8】

図 1 は、本発明の 1 つの実施の形態の認証決済システムの全体構成を示している。このシステムは、サービス提供（商品販売を含むものとする。以下同じ。）を行うサービス提供装置 1 0 3 と、このサービス提供装置 1 0 3 からサービス提供を受ける端末装置 1 0 2 と、サービス提供装置 1 0 3 及び端末装置 1 0 2 から信頼され、認証及び／又は決済処理を行うためのサービス証明書を発行する認証決済装置 1 0 1 と、端末装置の制御情報を生成及び／又は公開する制御情報提供装置 1 1 1 を備えている。

#### 【0 0 4 9】

これらの各装置はインターネットなどのネットワーク 1 0 0 を介して接続され、相互にデータの送受が可能となっている。ここでネットワーク 1 0 0 は有線に限らず電磁波など無線により実現されていても良い。さらにこれらの装置間のメ



ッセージの送受信はTCP/IP上でXMLプロトコル、SOAP、SMTPやHTTPのような伝送プロトコルを用いてのXMLベースのメッセージにより行う。けれどもこれらに限らず、これらと同等の機能を有する方式により実現されて良い。

#### 【0050】

このシステムを構成する各装置はそれぞれ環境104、106、108とネットワークへの接続などのポリシー105、107、109を持つ。この環境としては、例えば、端末装置の能力、接続ネットワークの種類・帯域、利用料金があり、ポリシーとしては、例えば、通信路上を送信するメッセージのセキュリティ強度への要求、料金への要求、応答速度がある。

#### 【0051】

認証決済装置101は決済機関などに設けられるもので、端末装置102を操作する利用者及び／又は端末装置102自体の信用管理、権限管理や属性情報管理を行うためのデータベース110を持っている。この認証決済装置101は、データベース110に登録されている信用情報、権限情報、属性情報等の情報に従ってサービス許可等の情報を含むサービス証明書を発行する。

#### 【0052】

制御情報提供装置111が生成及び／又は公開する制御情報には、端末装置102がサービス提供装置103に対してサービス要求を行う際のサービス要求手順及び／又はサービス要求メッセージフォーマットが記述されている。この制御情報提供装置111はサービス提供装置103が兼ねても良い。

#### 【0053】

認証決済装置101の構成について、図2を用いて説明する。図2において、201はネットワーク送受信部であり、ネットワークとのデータの入出力を司り、端末装置102やサービス提供装置103とのデータの送受信を行う。202は制御部であり、各部の制御、種々の演算、データの一時的な格納等を行う。203は認証決済処理部であり、顧客情報管理部204に含まれる顧客の属性情報、権限情報、決済情報、信用情報の更新を行う。205はサービス証明書生成部であり、顧客情報管理部204の情報を参照して端末装置102に対するサービ

ス証明書の発行を行う。206はポリシー・環境情報管理部であり、ここで認証決済装置101のポリシー管理、ネットワーク接続状況などを管理する。このポリシー・環境情報管理部206で管理される情報は、ネットワーク送受信部201、制御部202、認証決済処理部203、サービス証明書生成部205の動作に影響を与える。図2において、外部からポリシー・環境情報管理部206に入力される矢印は、環境情報の入力を意味する。

#### 【0054】

端末装置102の構成について、図3を用いて説明する。図3において、301はネットワーク送受信部であり、ネットワーク100とのデータの入出力を司り、認証決済装置101やサービス提供装置103とのデータの送受信を行う。ネットワーク接続は複数あっても良い。302は制御部であり、制御情報蓄積部303に収められた制御情報に基づき、各部の制御、種々の演算、データの一時的な格納等を行う。304は制御情報受信部であり、端末装置102を制御するための情報を受信した際に制御情報蓄積部303へそれを格納する。305は入出力部であり、液晶画面やキーボードなどに接続される。306はポリシー・環境情報管理部であり、ここで端末装置102や操作者のポリシーやネットワーク接続状況などを管理する。このポリシー・環境情報管理部306で管理される情報は、ネットワーク送受信部301、制御部302の動作に影響を与える。図3において、外部からポリシー・環境情報管理部306に入力される矢印は、環境情報の入力を意味する。

#### 【0055】

サービス提供装置103の構成について、図4を用いて説明する。図4において、401はネットワーク送受信部であり、ネットワーク100とのデータの入出力を司り、端末装置102や認証決済装置101とのデータの送受信を行う。402は制御部であり、制御情報蓄積部403に収められた制御情報に基づき、各部の制御、種々の演算、データの一時的な格納等を行う。404はサービス提供処理部であり、サービスの提供やコンテンツの配送処理等の処理を行う。405は認証決済要求生成部であり、認証決済装置101に対し認証決済処理を要求するためのメッセージを生成する。406は公開鍵キャッシュ部であり、電子署

名や暗号化処理において必要な公開鍵のキャッシュを行う。4 0 7 はポリシー・環境情報管理部であり、ここでサービス提供装置 1 0 3 や運営者のポリシーやネットワーク接続状況などを管理する。このポリシー・環境情報管理部 4 0 7 で管理される情報は、制御部 4 0 2 、サービス提供処理部 4 0 4 、認証決済要求生成部 4 0 5 の動作に影響を与える。図 4 において、外部からポリシー・環境情報管理部 4 0 7 に入力される矢印は、環境情報の入力を意味する。

#### 【 0 0 5 6 】

制御情報提供装置 1 1 1 の構成について、図 5 を用いて説明する。図 5 において、5 0 1 はネットワーク送受信部であり、ネットワーク 1 0 0 とのデータの入出力を司り、端末装置 1 0 2 やサービス提供装置 1 0 3 とのデータの送受信を行う。5 0 2 は制御部であり、各部の制御や種々の演算やデータの一時的な格納等を行う。5 0 3 は制御情報格納部であり、サービス提供装置 1 0 3 等の装置によって発行された端末装置 1 0 2 を制御するための情報が格納されており、ネットワーク送受信部 5 0 1 を介して受信した制御情報要求に応じて当該情報が送信される。5 0 4 はソフトウェア生成部であり、制御情報格納部 4 0 3 に収められた制御情報をもとにソフトウェアを生成する。5 0 5 はソフトウェアキャッシュ部であり、ソフトウェア生成部 5 0 4 にて生成されたソフトウェアをキャッシュしておく。これにより、一旦生成したソフトウェアと同一のソフトウェアが要求された場合の処理量を減少させることができる。なお、生成公開された制御情報には識別子や生成者の署名を付けても良く、この場合には制御情報の偽造を防止することが可能となる。

#### 【 0 0 5 7 】

上述した構成の制御情報提供装置 1 1 1 は、制御情報を生成及び／又は公開するための装置であり、端末装置 1 0 2 から Hyper Text Transfer Protocol (H T T P) のような情報取得プロトコルによる制御情報要求を受けて端末装置 1 0 2 に対して制御情報を送信する。この制御情報提供装置 1 1 1 が生成する制御情報には端末装置 1 0 2 がサービス提供装置 1 0 3 にサービスの要求を行う際のサービス要求手順やメッセージフォーマットが記述されている。端末装置 1 0 2 は、この情報に従って動作を行う。

**【 0 0 5 8 】**

当該制御情報は環境やポリシーといったような状況に応じて異なるサービス手順やメッセージフォーマットが用いられるような記述がなされており、状況に応じてサービス手順の変更や簡略化が行われる。制御情報の記述言語としては、例えば、Web Services Description Language (W S D L)、Web Services Flow Language (W S F L) を用いることができる。W S F L と W S D L の記述例の抜粋をそれぞれ図 6 及び図 7 に示す。

**【 0 0 5 9 】**

図 6 の記述例は、認証決済装置 1 0 1 が生成するサービス証明書に含まれる基準額と決済金額を比較して、決済金額がサービス証明書に含まれる基準額よりも小さい場合にはサービス提供を決済処理に先行して行い、そうでない場合は決済処理をサービス提供に先行して行う処理の記述である。

**【 0 0 6 0 】**

図 7 の記述例は、端末装置 1 0 2 とサービス提供装置 1 0 3 と間の接続ネットワーク 1 0 0 が赤外線 (I r D A) の場合には S S L を用いない接続を行い、それ以外の場合には S S L を用いた接続を行う処理の記述である。また、メッセージ "Service Assertion" には、XML 署名が付加される。ここで示した基準額やネットワーク環境の記述はあくまでも例であって限定されるものではない。例えば、位置など他の環境情報を用いても良く、環境情報に限らず端末装置利用者やサービス提供者の嗜好情報といったようなポリシーを使用しても良い。

**【 0 0 6 1 】**

また端末装置 1 0 2 は、前述の制御情報の取得において当該端末装置 1 0 2 の能力、例えば、S S L の利用可否、XML-Signature の利用可否、XML-Encryption の利用可否を制御情報提供装置 1 1 1 に通知し、制御情報提供装置 1 1 1 は、当該能力に合わせて制御情報の変更を行って端末装置 1 0 2 に送付するようにしても良い。この変更例としては、図 1 1 のような W S D L を端末装置に送信するのではなく、端末装置の持つ能力に合わせて W S D L 記述を生成し、図 2 0 のような W S D L 記述を端末装置に送信するなどがあげられる。ここでは、I r D A の能力を持たない端末装置に対して必ず S S L を用いるような W S D L 記述を生成

している。この際、端末装置からの能力は、例えばCC/PPを用いて通知される。CC/PP記述の例は図21に示す。

#### 【0062】

なお、端末装置102は上述した制御情報に基づいて動作する代わりに、制御情報相当の情報が含まれるソフトウェアを取得し、当該ソフトウェアにより所望の動作を実現するようにしても良い。またそのために、制御情報提供装置111が前述のソフトウェアを提供することにしても良い。さらに、ソフトウェアの生成においては、WSDL、WSFLで記述されたあらゆる機能を含めたソフトウェアにしても良いし、WSDL、WSFLを解釈し、装置の能力に合わせて必要な機能のみを備えるように生成しても良い。ここで、生成されるソフトウェアの言語としては例えばJ A V A（登録商標）を用いる。

#### 【0063】

次に、本実施の形態の認証決済システムとの動作を説明する。本システム、各装置におけるサービス手順とメッセージフォーマットは制御情報に応じて定まるものであり、処理の順序は特定の手順に必ずしも縛られるものではない。しかしながら、ここでは各装置の動作を説明するため、1つのサービス提供・要求方法を想定して、状況に適応したサービス提供・要求方法の変更を説明する。

#### 【0064】

図8に、各装置のメッセージの送受信時の手順を示す。この手順において、各装置はポリシー及び／又は環境に応じて、メッセージ送受信時のSecure Socket Layer（SSL）の適用・非適用、電子署名の適用・非適用、暗号化の適用・非適用、情報圧縮の適用・非適用などサービス提供方法の使い分けを行う。

#### 【0065】

ステップS101からS103において、ネットワークメッセージフォーマット情報から取得した接続ネットワークの種類と、SSL処理にかかる計算量と、決済の安全性を重視するか決済の速度を重視するかなどの顧客の嗜好情報とからセキュリティ強度の向上が必要か否かを判定する。ここでセキュリティ強度の向上が必要と判定した場合には、SSLによる接続を確立する。

#### 【0066】

これによって、端末装置 102 とサービス提供装置 103 と間の通信にインターネットが用いられる場合のようにセキュリティ強度の向上が必要な場合と、端末装置と 102 とサービス提供装置 103 と間の通信がごく近距離の赤外線を用いて行われる場合のようにセキュリティの保証が十分だと考えられるネットワークを用いる場合とで SSL の使用、不使用を切り分け、セキュリティが不十分なネットワークにおけるセキュリティの確保、セキュリティが十分なネットワークにおける処理の高速化が図れる。

#### 【0067】

ステップ S104 において送信メッセージの生成を行う。ステップ S105 から S106 においては、ネットワークの接続速度情報や、情報の一部を送信した場合と情報全体を送信した場合とのデータ量の比較結果から、部分情報の送信で良いか全体情報の送信が必要かを判定し、全体情報の送信不要と判定した場合、必要情報のみの抽出処理や前回送信した情報との差分情報の抽出処理によりデータ生成を行う。これによって、伝送情報の量を減らすことができ、処理時間の短縮が図れる。

#### 【0068】

ステップ S107 から S108 において、端末装置 102 の機能と、サービス提供装置 103 や顧客のポリシーから XML 署名の付加が必要か否かを判定し、付加が必要と判定した場合には、メッセージに XML 署名を付加する。

#### 【0069】

これは、例えば、耐タンパ性を持つ端末装置と信頼性があるネットワークを用いる場合には電子署名を付加せずとも端末装置利用者の否認防止を図ることができるため、電子署名を付加しないことによって処理時間の短縮を図り、耐タンパ性を持たない端末装置や信頼性のない伝送路を用いる場合には電子署名を付加して否認防止を図るという使い分けが可能となる。

#### 【0070】

ステップ S109 と S110 において、接続ネットワーク 100 の種類と、端末装置 102 の計算能力、サービス提供装置 103、端末装置 102 の嗜好とから XML 暗号化が必要か否かを判定し、XML 暗号化が必要と判定した場合には

メッセージのXML暗号化を行う。これによってメッセージの一部分のみ暗号化するなどのXMLレベルでのセキュリティ強度を使い分けることができる。

#### 【0071】

ステップS111とS112において、生成したメッセージのXML圧縮の切替を行う。この処理によってXMLレベルでの情報量を減少させることができ、伝送速度が小さい場合の伝送時間の短縮が図れる。

#### 【0072】

なお、図8に示した手順は例であり、セキュリティの確保にあたってはSSL、XML署名やXML暗号化の使用に限定されるものではない。

#### 【0073】

図9に端末装置102のサービス提供装置103に対するサービス要求手順を示す。S201において、端末装置102は認証決済装置101からサービス証明書を受信する。これは必ずしもサービス要求時に行う必要はなく、事前に行っていても良く、また、端末装置102が認証決済装置101にサービス要求証明書を要求することにより受信しても、認証決済装置101が自発的に端末装置102に送信しても良い。

#### 【0074】

S202において、端末装置102は制御情報を制御情報提供装置111から取得する。これは必ずしもサービス要求時に行う必要はなく、事前に取得しておいても良い。また、制御情報の取得は明確な形で行う必要はなく、商品選択メニュー送受信メッセージ中に含めておいても良い。さらに定型的な制御情報を端末装置102の中に予め備えておいて、取得不要としても良い。また制御情報がソフトウェアの形式で公開される場合は、ソフトウェアの形式で取得することとして良い。

#### 【0075】

S203において、サービス提供装置103に対するサービス要求内容と認証決済装置101の発行したサービス証明書とを結合し、サービス提供装置103に送信するための図10に示すようなサービス証明書120を生成する。サービス要求内容には当該端末ユーザの識別子を含める。この識別子は認証決済装置1

0 1 発行のサービス証明書の識別子と同一の識別子を用いるものとする。

#### 【0 0 7 6】

ここで端末装置 1 0 2 は、制御情報提供装置 1 1 1 から受信した制御情報記述に従って、サービス証明書の一意性と信頼性が通知できる情報や、決済に必要な情報としてサービス証明書の識別子、サービス証明書を発行した認証決済装置 1 0 1 の識別子、認証決済装置 1 0 1 が付加した電子署名、基準額情報のようなサービス証明書の一部を抽出してその一部のみ送信したり、決済金額に応じて処理方法を変更するなど、このサービス証明書の内容、ポリシー、環境に応じてサービス手順の変更を行っても良い。端末装置が署名を付加する場合における署名者の識別子は、認証決済装置発行のサービス証明書の識別子と同じものを用いるものとする。

#### 【0 0 7 7】

環境やポリシーに応じてサービス要求方法が異なる場合は、サービス要求メッセージに接続ネットワーク情報など環境やポリシーに関する状況情報を付加してサービス提供装置 1 0 3 に送信しても良い。これにより、サービス提供装置 1 0 3 に端末装置 1 0 2 の状況を通知することができる。

#### 【0 0 7 8】

S 2 0 4 において、このようにして生成したサービス証明書 1 2 0 をサービス提供装置 1 0 3 に送信する。S 2 0 5、S 2 0 6 において、端末装置 1 0 2 はサービス提供装置 1 0 3 からサービスや商品を受け取り、領収書を受領する。

#### 【0 0 7 9】

図 1 7 のように、携帯電話網と無線 LAN、携帯電話網と有線 LAN と赤外線など、複数のネットワークインタフェースを持つ端末装置において、いずれのインタフェースを用いてもサービス提供装置に接続できる場合は、利用ネットワークの選択に、各ネットワークの特性情報や当該端末装置のポリシーや環境情報を用いても良い。

#### 【0 0 8 0】

ネットワークの特性情報は、図 1 7 のそれぞれのインタフェースに対して、例えば図 1 8 のようにネットワークの帯域やセキュリティ能力などの情報が記述さ



れる。この特性情報はネットワークインタフェースから取得されても、ネットワーク側から通知されても良い。また、ネットワーク情報としては、アクセスネットワーク情報に限定されず、エンド・ツー・エンドでの情報が示されても良く、さらに動的に変化しても良い。端末装置のポリシーは、例えば図19に示すように記述され、ここではユーザのネットワークの帯域、セキュリティ及び料金に対する嗜好情報が記述されている。使用ネットワークインタフェースの選択は、図18と図19に示される情報を評価することによって行い、例えば、 $(bandwidth \text{ に対するパラメータ}) \times 0.2 + (security \text{ に対するパラメータ}) \times 0.6 + 20 / (cost \text{ に対するパラメータ})$  のように評価でき、この場合、それぞれの値は、携帯電話機の場合は48.5、無線LANの場合は27、IrDAの場合は64のように評価され、最も値の大きなIrDAが選択されることになる。なお、評価に当たっては必ずしもこの式に限定されず、重み付けされて評価されても良い。

#### 【0081】

図11、図12及び図13にサービス提供装置103の端末装置102に対するサービス提供の手順と認証決済装置101に対する認証決済要求の手順を示す。S301において、サービス提供装置103は端末装置102からサービス要求内容と認証決済装置発行のサービス要求メッセージを受信する。

#### 【0082】

S302において、サービス提供装置103はサービス要求メッセージ中のサービス証明書120に含まれる認証決済装置101の署名やサービス証明書の有効期間を検証し、サービス証明書120の正当性を確認した後、端末装置102の状況を判定して適切なサービス提供フロー及びサービス提供メッセージフォーマットを選択する。

#### 【0083】

サービス証明書120の一意性と信頼性が通知できる情報として、サービス証明書の識別子、サービス証明書を発行した認証決済装置の識別子、認証決済装置が付加した電子署名のようにサービス証明書的一部分のみ抽出して端末装置102から送られてきた場合で、それらの情報だけでサービス提供手順が定まらない

場合は、認証決済装置 101 に当該データの内容問い合わせを行っても良い。

#### 【0084】

サービス証明書 120 に付加された電子署名の検証の際、サービス提供装置 103 は認証決済装置 101 の公開鍵証明書が必要になるが、事前にサービス提供装置 103 内にキャッシュしておけば公開鍵証明書の取得にかかる時間を短縮することが可能となる。

#### 【0085】

S303 において、サービス証明書 120 に含まれる基準額情報とサービス要求対象の決済額とを比較する。

#### 【0086】

このステップ S303 において、決済額が基準額よりも大きい場合は認証決済メッセージを生成して認証決済装置 101 に送信する（ステップ S304）。そして決済処理が成功した後にサービス提供を開始し（ステップ S305）、領収書の送付を行う（ステップ S306）。

#### 【0087】

他方、ステップ S303 において、基準額が決済額よりも大きい場合は、認証決済要求の生成に先立ちサービス提供を開始する（ステップ S307）。ここで決済金額が非常に小さい場合は処理の簡略化を行っても良い。例えば、まとめて決済認証処理を行う（ステップ S308 及び S311）。これにより利用金額が小さい場合の決済費用を圧縮することが可能となる。そうでない場合は、サービスを提供する毎に認証決済要求を生成して認証決済装置 101 に当該メッセージを送信し（ステップ S309）、領収書の送付を行う（ステップ S310）。

#### 【0088】

以上の手順により、決済金額に応じてサービス開始を早めることができ、利用金額が高く決済リスクが比較的大きい場合は決済処理を確実に行うことができる。なお、ここで状況に適應してサービス順序を変更するだけでなく、処理の簡略化を行ったりしても良い。

#### 【0089】

コンテンツ配信を行う場合においては、サービス要求後直ちにコンテンツ配信

を開始すると同時に認証決済処理を行い、認証決済処理に失敗した場合は、コンテンツ配信を終了するという実現形式でも良い。

#### 【0090】

図12ではサービス提供装置103から認証決済装置101に対する認証決済要求手順を示している。サービス提供装置103は、端末装置102から受信したサービス証明書120を解析し、必要な情報の抽出、決済金額などを付加して認証決済要求を生成し（ステップS401）、当該認証決済要求を認証決済装置101に送信し（ステップS402）、その後応答を受信する（ステップS403）。

#### 【0091】

認証決済の送信において、サービス証明書120の一意性と信頼性が通知できる情報として、サービス証明書の識別子、サービス証明書を発行した認証決済装置101の識別子、認証決済装置101が付加した電子署名等、サービス証明書120の一部を送信しても良い。

#### 【0092】

図13ではサービス提供装置103への一括認証決済手順を示している。この処理では、サービス要求を受け取る度に毎回認証決済処理を行うのではなく、適当な規則に従って数回分の認証決済処理を一括して行う。このための規則としては、例えば、L. Rivest著の[“Electronic Lottery Tickets as Micropayments”, in Financial Cryptography: FC '97, Proceedings, R. Hirschfeld (ed.), Springer-Verlag, LNCS vol. 1318, pp. 307-314, 1998]に示されるような方法による確率的な処理があげられる。

#### 【0093】

ステップS501では認証決済要求を行うかどうかを判定し、行う場合には蓄積済みの認証決済情報を読み出し（ステップS502）、認証決済要求を生成して認証決済装置101に送信し（ステップS503）、当該処理が成功したら端末装置102に対して領収書の送付を行う（ステップS504）。

#### 【0094】

ステップS501で認証決済要求の送信を行わないと判定した場合には、当該

認証決済情報の蓄積を行い、別の機会の認証決済要求送信に備える（ステップ S 5 0 5）。

#### 【 0 0 9 5 】

認証決済装置 1 0 1 は他の装置からの要求を受けて、認証や決済に関連して図 1 0 に示したようなサービス証明書 1 2 0 の発行や決済などの処理と利用者の属性情報、信用情報、決済情報、認証情報などの情報の管理を行う。図 1 4 に認証決済装置 1 0 1 のサービス証明書発行手順、認証決済要求処理手順を示す。

#### 【 0 0 9 6 】

ステップ S 6 0 1 において、認証決済装置 1 0 1 が他の装置から何らかの要求を受ければ、サービス証明書の要求を受けたのか、認証決済の要求を受けたのかに応じて処理を分岐する（ステップ S 6 0 2）。

#### 【 0 0 9 7 】

ここでサービス証明書の要求を受けた場合、当該認証決済装置 1 0 1 が管理する端末装置 1 0 2 に関する情報に基づいてサービス証明書 1 2 0 を生成する（ステップ S 6 0 3）。生成されたサービス証明書 1 2 0 は認証決済装置 1 0 1 の署名を付けて端末装置 1 0 2 に送信される（ステップ S 6 0 4）。

#### 【 0 0 9 8 】

このサービス証明書に含めるべき情報の全部又は一部を蓄積装置 1 1 0 に蓄積しておき、サービス証明書本体には当該蓄積情報の蓄積位置を示すこととしても良い。ここでサービス証明書 1 2 0 には基準額情報が含まれるものとする。なお、この基準額情報は、当該サービス証明書 1 2 0 に示される基準額以下の商品をサービス提供装置 1 0 3 が提供する場合に、決済処理に先行してサービス提供を開始して良いことを認証決済装置 1 0 1 が保証することを意味するものとする。

#### 【 0 0 9 9 】

ステップ S 6 0 2 で認証決済要求を受けた場合は、認証決済処理を行い（ステップ S 6 0 5）、必要があれば管理下にある情報の更新を行い（ステップ S 6 0 6）、処理が成功したのか失敗したのかを示す結果を送信する（ステップ S 6 0 7）。

#### 【 0 1 0 0 】

管理下にある情報が更新されることによって、サービス証明書 120 を更新する必要がある場合は、ステップ S608 からステップ S603 に進み、端末装置 102 に対してサービス証明書 120 の発行を行う。なお、サービス証明書 120 に対する記載内容としては、必ずしも当該基準額情報に限定されるわけではなく、利用上限回数や年齢情報その他の認証情報、サービス許可情報や属性情報であって良い。

#### 【0101】

図 15 に認証決済装置 101 が端末装置 102 に発行するサービス証明書 120 の記述例を示す。この例において、サービス証明書 120 は Security Assertion Markup Language (SAML; <http://www.oasis-open.org/committees/security/>) を用いて記述しているが、同様の記述が可能であればこの限りではない。また、サービス証明書 120 には有効期間、認証決済装置識別子及び一意的な識別子が付与されるものとし、サービス証明書の有効性の記述や再利用検出を可能とする。

#### 【0102】

決済処理に関しては前払いとしても後払いとしても良い。また、認証決済装置 101 はサービス証明書 120 を端末装置 102 の要求に応じて発行しても、端末装置 102 の要求なしに発行しても、周期的に発行するなど任意の時点で更新しても良い。またサービス証明書 120 は 1 回のみ利用可能としても、複数回利用可能としても良く、1 つの端末装置 102 に複数の証明書を発行しても良い。

#### 【0103】

なお、複数回利用可能とする場合、図 16 に示すように、端末装置 102 から受信したサービス証明書に対し（ステップ S701）、基準額を減額して（ステップ S702）、サービス提供装置 103 の電子署名を付加して（ステップ S703）、端末装置 102 に送り返すことによって更新するようにしても良い（ステップ S704）。

#### 【0104】

ここで、サービス証明書が複数回利用されても良く、またサービス提供装置 103 が一括決済処理を行う場合、認証決済装置 101 はサービス証明書の利用状

況を完全に把握することができないため、端末装置 102 の利用者の支払い能力を超えた利用が行われる可能性がある。

#### 【0105】

この課題を解決するため、サービス証明書には当該サービス証明書による利用可能な金額の最大値及び／又は最大利用回数を示しておき、端末装置 102 は当該サービス証明書の利用履歴を管理し、当該最大利用金額又は最大利用回数を超えた場合に認証決済装置 101 に通知し、サービス証明書の更新処理を行うようにしても良い。さらにこの場合に、端末装置 102 は認証決済装置 101 に最大利用金額又は最大利用回数を通知する際、最大利用金額又は最大利用回数を超えたことを通知するだけでなく、当該サービス証明書の利用履歴を認証決済装置 101 に送付し、認証決済装置 101 の管理下の情報の更新を行っても良い。このような処理方式にすれば、認証決済装置 101 が負うリスクを軽減することができる。

#### 【0106】

##### 【発明の効果】

以上のように本発明によれば、サービス証明書に記載された顧客の利用可能金額、通信路のセキュリティ強度、伝送帯域、位置などの環境やポリシーなどの状況に適応して暗号化、署名の付加などサービス手順及び／又はメッセージフォーマットを適応的に使い分けることにより、サービス提供時間の短縮化、セキュリティ強度の調節、伝送情報の削減等を行うことができる。

#### 【0107】

またすべての情報を暗号化、署名付与するのではなく、一部分を暗号化、署名付与することにより、重要部分のみ暗号化することも可能である。

#### 【0108】

さらにこれらのメッセージの一部をメッセージ本文に含めるのではなくて蓄積装置に蓄積し、メッセージ本文には当該蓄積装置への蓄積位置への参照情報を含めることによって伝送情報の量を削減することができる。これは特に、利用率が低い情報の添付に特に有効である。

#### 【0109】

本発明によればまた、端末装置及びサービス提供装置から信頼された認証決済装置が端末装置に対し、サービス提供装置が認証、サービス許可、決済を行う上での信用情報、補助情報を含むサービス証明書を署名付きで発行し、端末装置が認証決済装置の発行した当該署名付きサービス証明書に情報の付加を行ってサービス提供装置に送信するので、認証決済装置が顧客を保証し、サービス提供装置はリスクが小さな場合にサービス証明書の署名検証による正当性を確認するのみにしてサービス提供を行い、このサービス提供を複雑な認証、サービス許可や決済処理に先行して行うことができる。

#### 【0110】

また、サービス証明書を転送する際に必須情報のみ抽出して送信することにより、伝送情報を削減することができる。

#### 【0111】

また、サービス提供装置が端末装置から受信したサービス証明書に情報の付加を行って認証決済装置に送信することにより、認証決済装置において顧客情報の更新、決済処理を行い、サービス証明書の内容更新に繋げることができる。

#### 【0112】

さらに認証決済装置が顧客情報の更新を契機にサービス証明書を端末装置に送信したり、定期的にサービス証明書を更新したりすることによって、端末装置は常に最新の情報を反映したサービス証明書を保持することができ、これによって、サービス提供装置のリスクを減少させることができる。

#### 【0113】

本発明によればまた、端末装置が、状況に適應する制御情報を生成し公開する装置からサービスフローやメッセージフォーマットのようなサービスインタフェースを取得し、それに従って動作することにより、状況に適應して柔軟なサービス要求を行うことができる。

#### 【0114】

また当該サービスインタフェース記述に一意的な識別子を付与することにより、当該識別子によりサービスインタフェースを同定できるようになり、同一のインタフェースを用いるサービスを利用する場合に、再度当該サービスインタフェ

ースをダウンロードする回数を減少させることができる。

【0115】

さらに、制御情報提供装置が当該サービスインタフェースに電子署名を行うことにより、当該サービスインタフェースの否認防止、完全性保証を行うことができる。

【0116】

またさらに、当該サービスインタフェース情報をもとに端末装置で動作するソフトウェアを生成し、端末装置上で動作させることにより、端末装置が必ずしも当該サービスインタフェース記述を理解して動作する必要性をなくすことができ、また、端末装置の機能に合わせたソフトウェアを生成することにより、当該ソフトウェアのサイズを減少させることができ、伝送情報量、端末装置における記憶領域使用量を削減することができる。

【0117】

さらに、制御情報提供装置において生成したソフトウェアをキャッシュし、同一のソフトウェアを要求された場合に当該キャッシュから読み出し送信を行うことにより、当該ソフトウェアの生成コストの削減、時間の短縮が図れる。

【図面の簡単な説明】

【図1】

本発明の1つの実施の形態のシステムの全体構成を示すブロック図。

【図2】

上記実施の形態における認証決済装置の構成を示すブロック図。

【図3】

上記実施の形態における端末装置の構成を示すブロック図。

【図4】

上記実施の形態におけるサービス提供装置の構成を示すブロック図。

【図5】

上記実施の形態における制御情報提供装置の構成を示すブロック図。

【図6】

上記実施の形態におけるサービス手順の記述例のプログラムリスト。



**【図 7】**

上記実施の形態におけるメッセージフォーマットの記述例のプログラムリスト。  
。

**【図 8】**

上記実施の形態におけるメッセージの送受信時の手順を示すフローチャート。

**【図 9】**

上記実施の形態における端末装置のサービス提供装置に対するサービス要求手順を示すフローチャート。

**【図 1 0】**

上記実施の形態において端末装置からサービス提供装置に送信されるサービス証明書の説明図。

**【図 1 1】**

上記実施の形態におけるサービス提供装置の端末装置に対するサービス提供手順と認証決済装置に対する認証決済要求手順の一例を示すフローチャート。

**【図 1 2】**

図 1 1 のフローチャートにおける認証決済要求処理の詳細手順を示すフローチャート。

**【図 1 3】**

図 1 1 のフローチャートにおける一括認証決定要求処理の詳細手順を示すフローチャート。

**【図 1 4】**

上記実施の形態における認証決済装置のサービス証明書発行手順、認証決済要求処理手順を示すフローチャート。

**【図 1 5】**

上記実施の形態におけるサービス証明書の記述例のプログラムリスト。

**【図 1 6】**

図 1 4 のフローチャートにおけるサービス証明書の更新処理の詳細手順を示すフローチャート。

**【図 1 7】**

複数種のネットワークインタフェースをもつ端末装置装置の構成図。

【図 1 8】

ネットワークの帯域、セキュリティ能力などの特性情報の記述例のプログラムリスト。

【図 1 9】

端末装置のポリシーの記述例のプログラムリスト。

【図 2 0】

W S D L の記述例のプログラムリスト。

【図 2 1】

C C / P P 記述例のプログラムリスト。

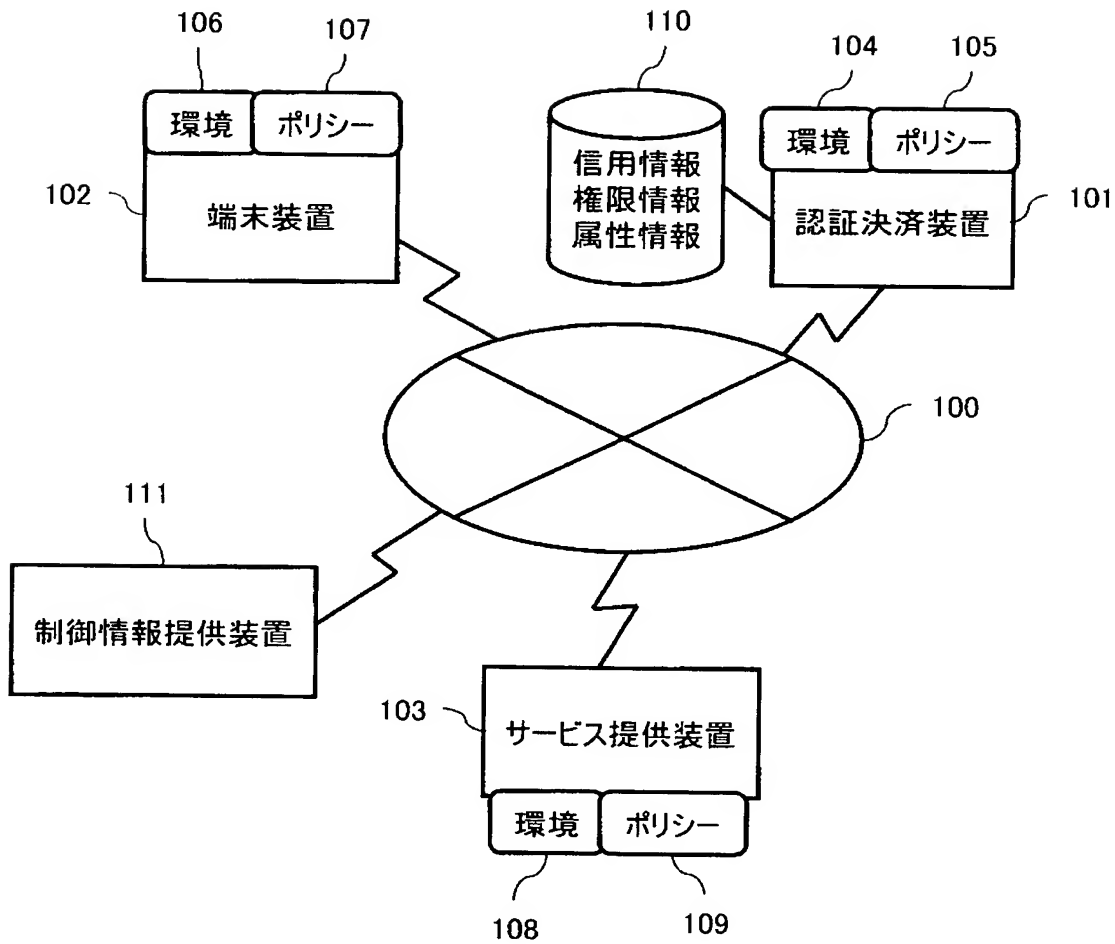
【符号の説明】

- 1 0 0 ネットワーク
- 1 0 1 認証決済装置
- 1 0 2 端末装置
- 1 0 3 サービス提供装置
- 1 1 1 制御情報提供装置
- 2 0 1 ネットワーク送受信部
- 2 0 2 制御部
- 2 0 3 認証決済処理部
- 2 0 4 顧客情報管理部
- 2 0 5 サービス証明書生成部
- 2 0 6 ポリシー・環境情報管理部
- 3 0 1 ネットワーク送受信部
- 3 0 2 制御部
- 3 0 3 制御情報蓄積部
- 3 0 4 制御情報受信部
- 3 0 5 入出力部
- 3 0 6 ポリシー・環境情報管理部
- 4 0 1 ネットワーク送受信部

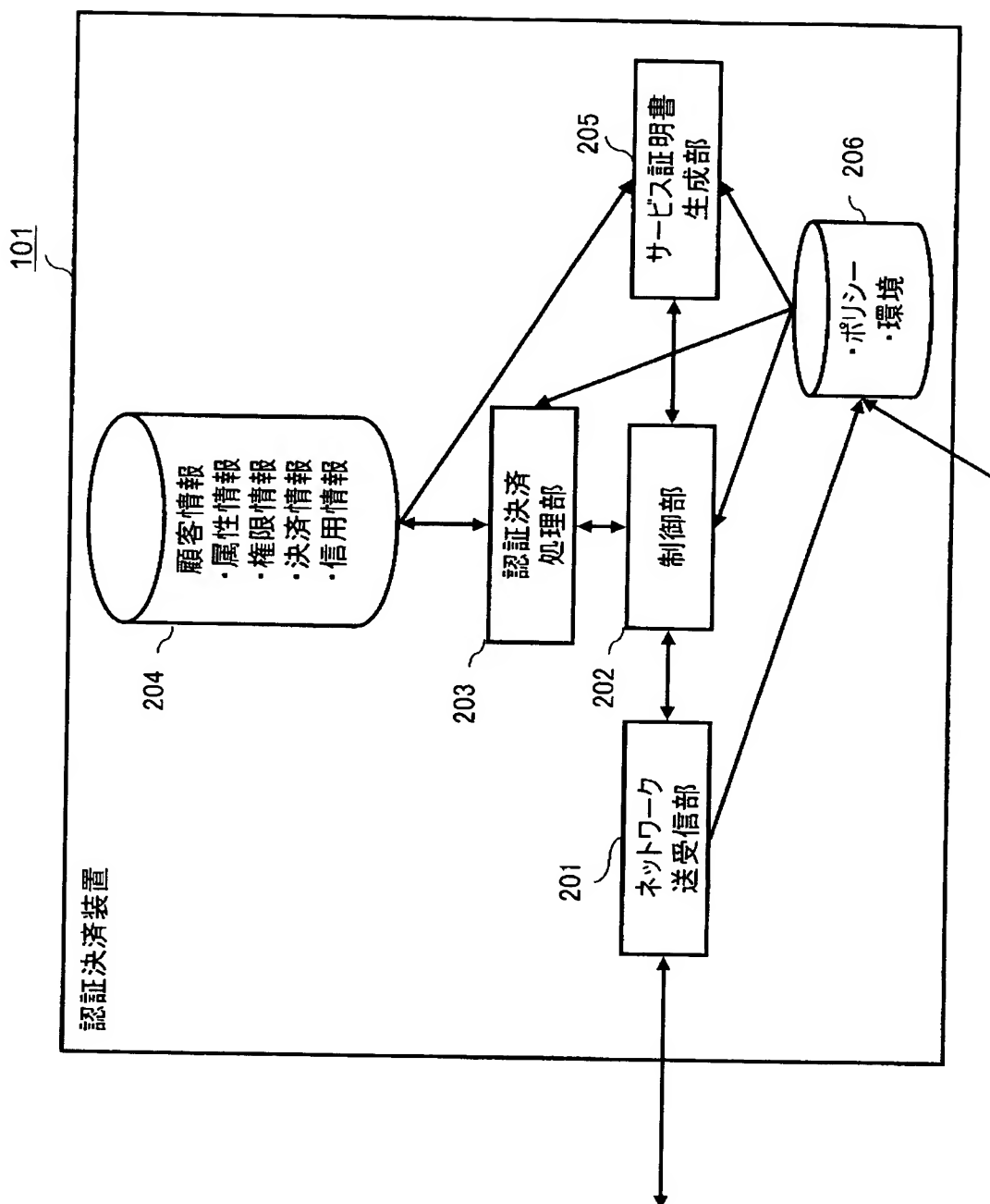
- 4 0 2 制御部
- 4 0 3 制御情報蓄積部
- 4 0 4 サービス提供処理部
- 4 0 5 認証決済要求生成部
- 4 0 6 公開鍵キャッシュ部
- 4 0 7 ポリシー・環境情報管理部
- 5 0 1 ネットワーク送受信部
- 5 0 2 制御部
- 5 0 3 制御情報格納部
- 5 0 4 ソフトウェア生成部
- 5 0 5 ソフトウェアキャッシュ部

【書類名】 図面

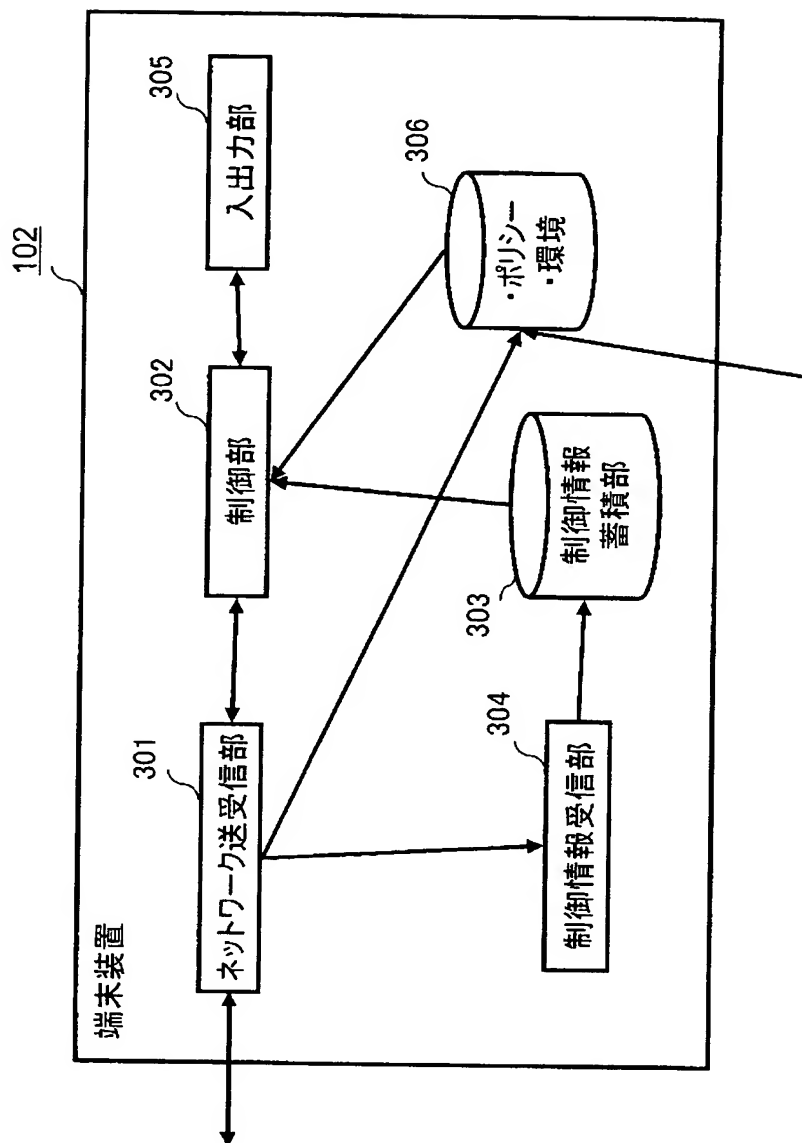
【図 1】



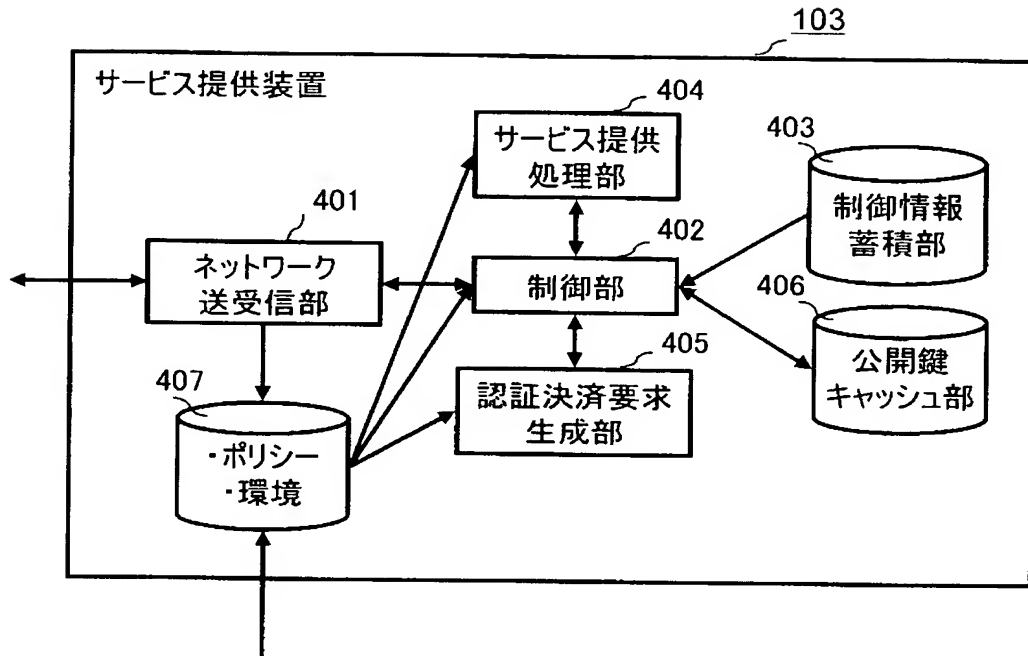
【図 2】



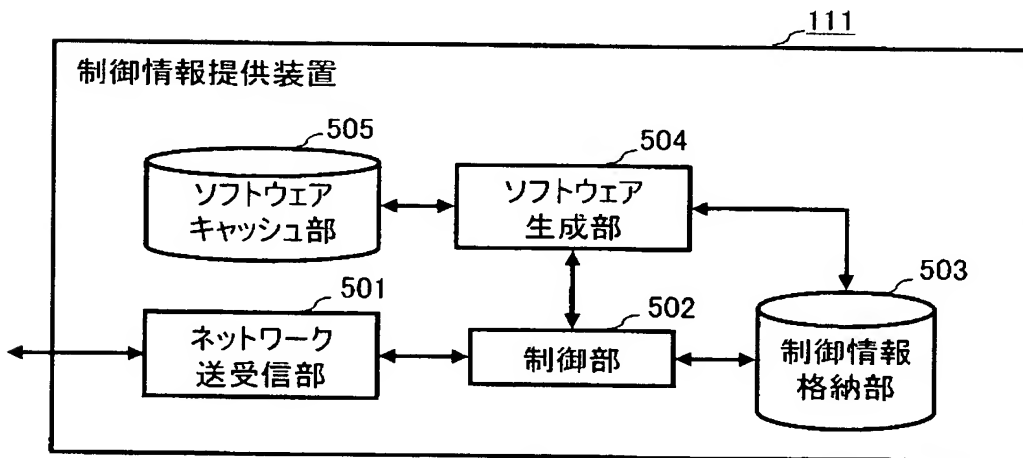
【図 3】



【図 4】



【図 5】



【図 6】

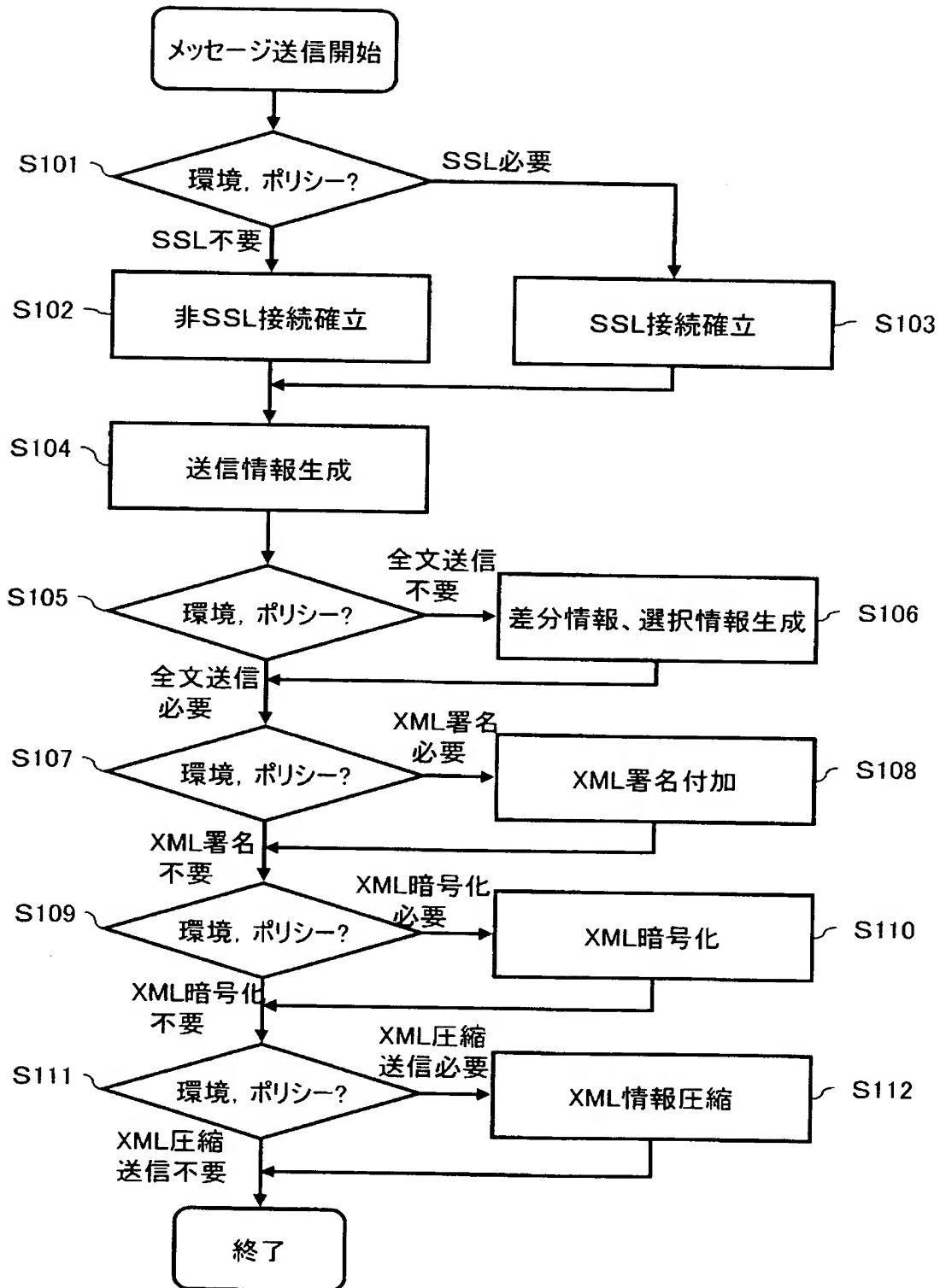
```
<flowModel name="ServiceProvider" ...>
  <flowSource name="getOrder" .../>
  <activity name="flowSelection" .../>
  <activity name="SendETicket" .../>
  <activity name="requeStCharge" .../>
  <activity name="receiveConfirmation" .../>
  <activity name="SendReceipt" .../>
  <controllink
    Source="getOrder" target="SendETicket"
    tranSitionCondition="....my:amount >= ....price"/>
  <controllink
    Source="SendETicket" target="requeStCharge"
    tranSitionCondition="....my:amount >= ....price"/>
  <controllink
    Source="requeStCharge" target="receiveConfirmation"/>
  <controllink
    Source="receiveConfirmation"
    target ="SendReceipt"
    tranSitionCondition="....my:amount >= ....price"/>
  <controllink
    Source="getOrder" target="requeStCharge"
    tranSitionCondition="....my:amount < ....price"/>
  <controllink
    Source="requeStCharge" target="receiveConfirmation"/>
  <controllink
    Source="receiveConfirmation" target="SendETicket"
    tranSitionCondition="....my:amount < ....price"/>
  <controllink
    Source="SendETicket"
    target ="SendReceipt"
    tranSitionCondition="....my:amount < ....price"/>
</flowModel>
```



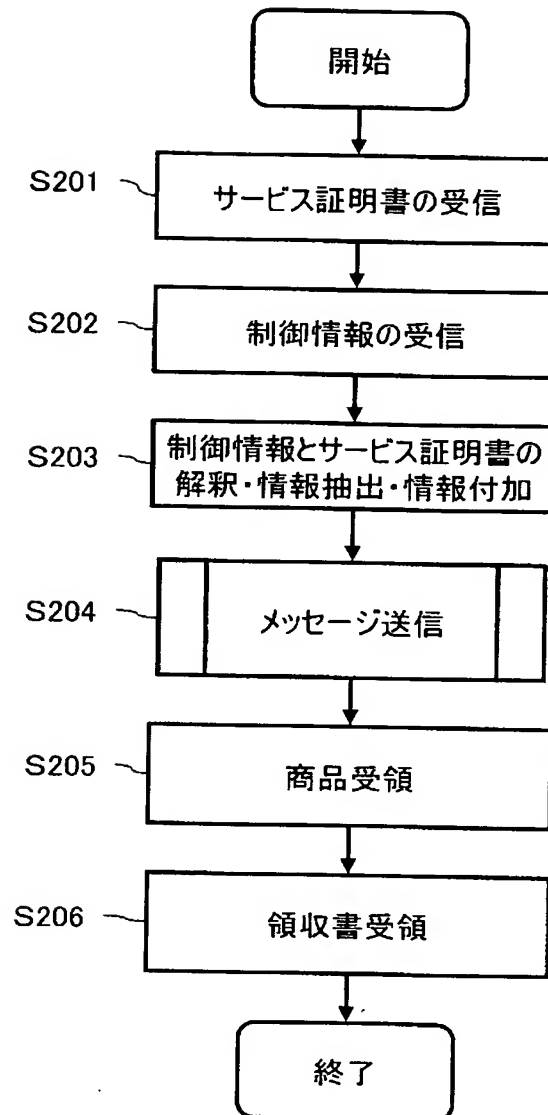
## 【図 7】

```
<definitionS xmlns:dS="http://www.w3.org/2000/09/xmldSig#" ...>
  <typeS .../>
  <message name="getOrderInput">
    <part name="getOrderRequest"
      type="tn:getOrderType"
      dS:algorithm=
        "http://www.w3.org/2000/09/xmldSig#rsa-sha1"/>
      <part name="ServiceAsserion" type="Saml:Asserion"
        dS:algorithm=
          "http://www.w3.org/2000/09/xmldSig#rsa-sha1"/>
    </message>
  <portType .../>
  <binding .../>
  <Service name="getService">
    <port name="placeOrder"
      binding="tn:placeOrderPortBinding">
      <ext:Switch>
        <ext:case>
          <ext:condition>
            <ext:access>IrDA</ext:access>
          </ext:condition>
          <ext:action>
            <Soap:address
              location="http://example1.com/provider"/>
            </ext:action>
          </ext:case>
          <ext:default>
            <ext:action>
              <Soap:address
                location="httpS://example1.com/provider"/>
            </ext:action>
          </ext:default>
        </ext:Switch>
      </port>
    </Service>
  </definitionS>
```

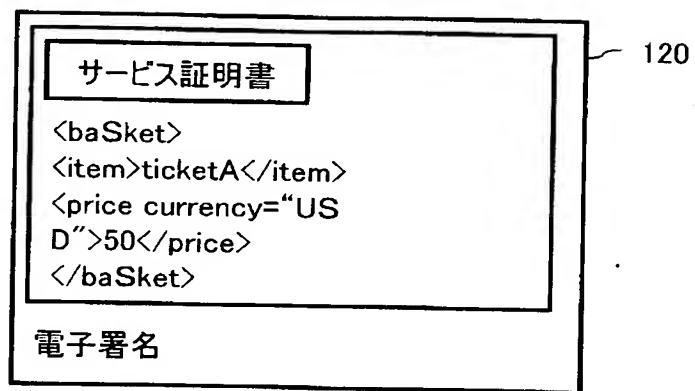
【図 8】



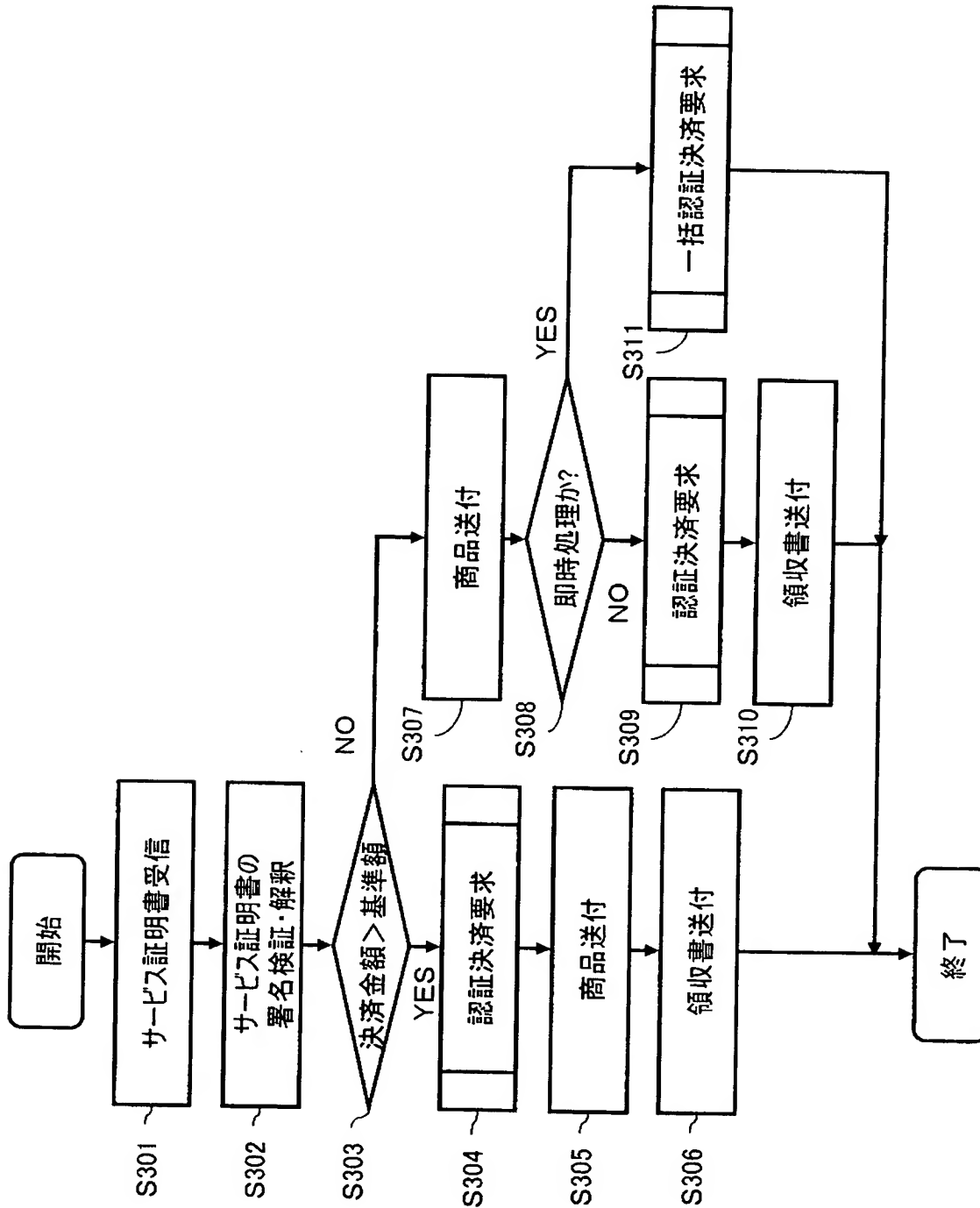
【図 9】



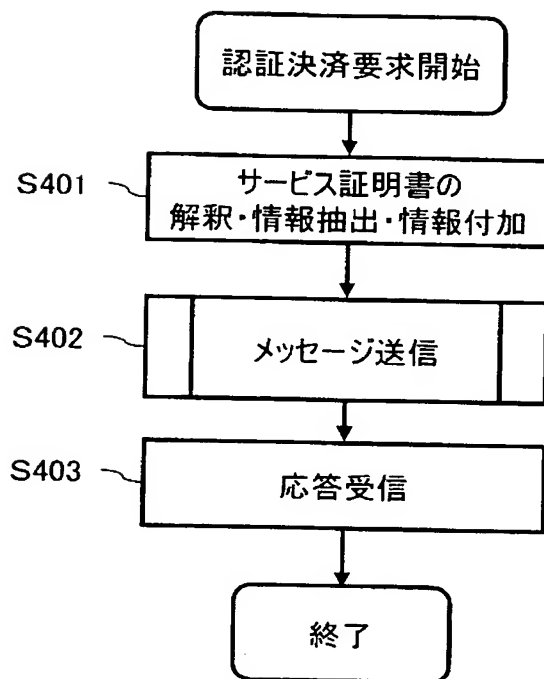
【図 10】



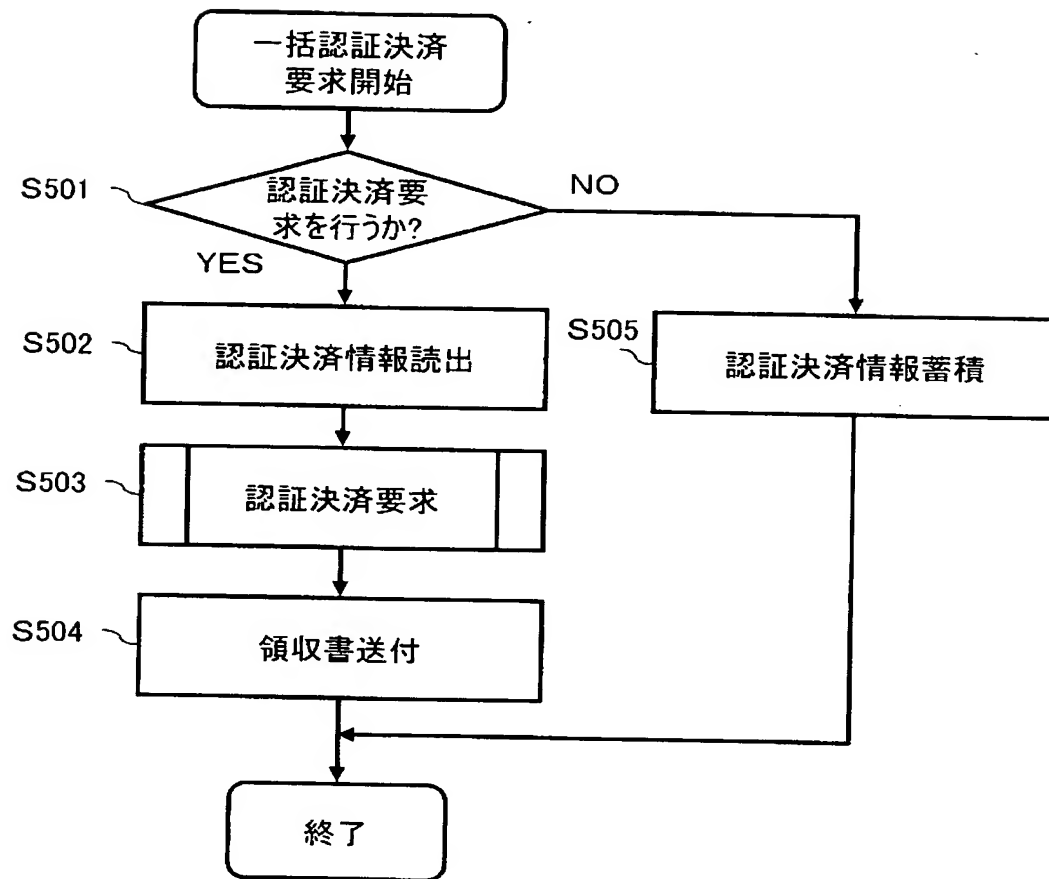
【図 11】



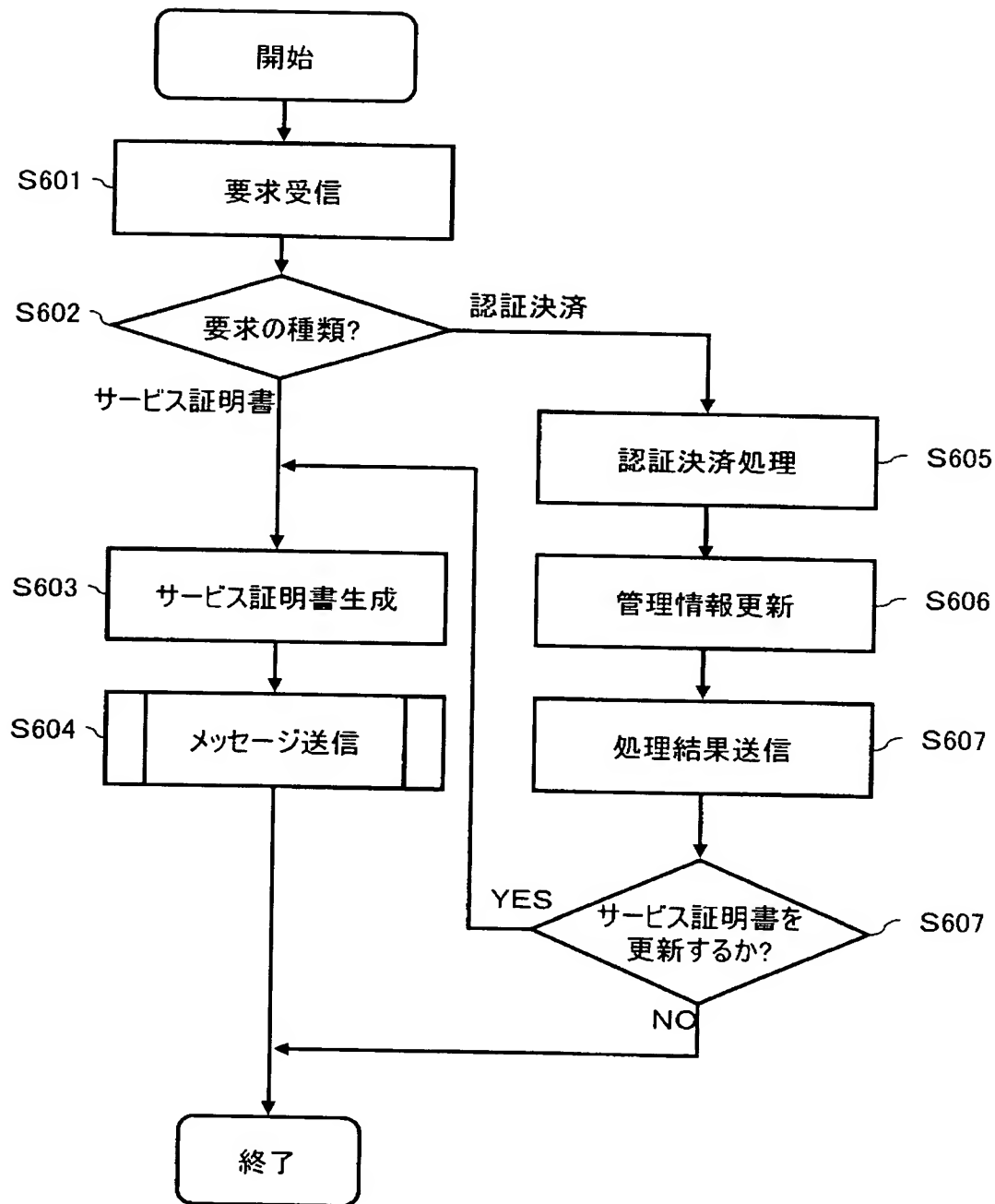
【図 12】



【図 13】



【図 14】

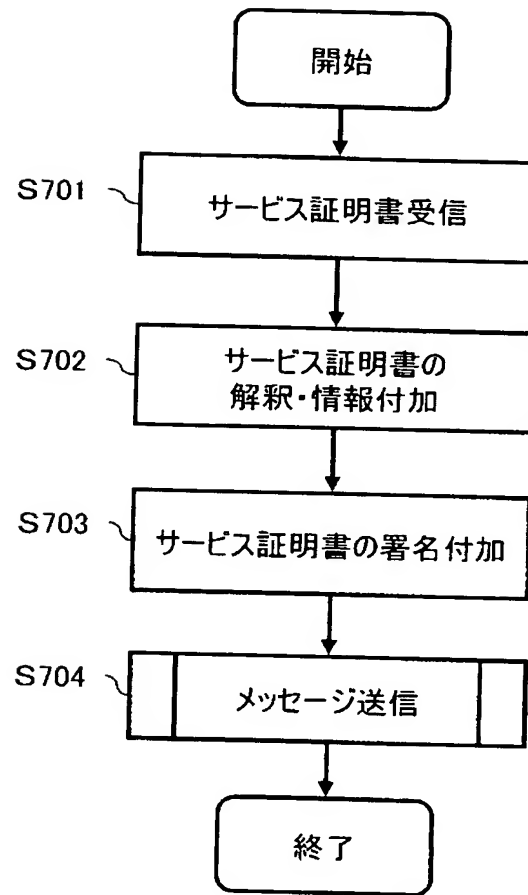




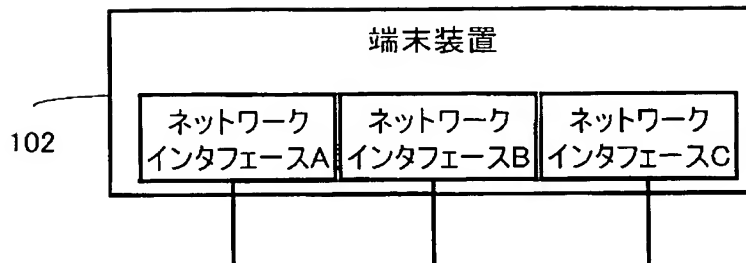
【図 15】

```
<Saml:ASSertion
MajorVerSion="1" MiNOVerSion="0"
ASSertionID="192.168.0.1.12345678"
ISSuer="NTT DoCoMo, Inc."
ISSueInStant="2002-08-01T10:09:35Z">
<Saml:ConditionS
NOtBefore="2002-08-01T10:00:00Z"
NOtAfter="2002-08-03T10:00Z"/>
<Saml:AttributeStatement>
<Saml:Subject>
<Saml:NameIdentifier
SecurityDomain="docomo.ne.jp"
Name="uSer1"/>
</Saml:Subject>
<Saml:Attribute
AttributeName="LimitWithoutAuthorization"
AttributeNameSpace="http://nttdocomo.ne.jp">
<Saml:AttributeValue>
<my:amount currency="USD">
500
</my:amount>
<Reference URI="http://nttdocomo.co.jp/repoSitory/uSer1/Saml.xml"/>
<my:SecretValue>
<EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#Content">
<CipherData>
<CipherValue>A23B45C56</CipherValue>
</CipherData>
</EncryptedData>
</my:SecretValue>
</Saml:AttributeValue>
</Saml:Attribute>
</Saml:AttributeStatement>
</Saml:ASSertion>
```

【図 16】



【図 1 7】



【図 1 8】

```

<networkDescription>
<access>mobile phone</access>
<bandwidth>1</bandwidth>
<securityStrength>80</securityStrength>
<cost>80</cost>
</networkDescription>

```

```

<networkDescription>
<access>wireless LAN</access>
<bandwidth>100</bandwidth>
<securityStrength>10</securityStrength>
<cost>20</cost>
</networkDescription>

```

```

<networkDescription>
<access>IrDA</access>
<bandwidth>10</bandwidth>
<securityStrength>70</securityStrength>
<cost>1</cost>
</networkDescription>

```

【図 1 9】

```
<userprofile>
<preference>security=0.6,bandwidth=0.2,cost=0.2</preference>
</userprofile>
```

【図 2 0】

```
<definitions
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" ...>
<types .../>
<message name="getOrderInput">
<part name="getOrderRequest"
type="tns:getOrderType"
ds:algorithm=
"http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<part name="serviceAssertion"
type="saml:Assertion"
ds:algorithm=
"http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
</message>
<portType .../>
<binding .../>
<service name="getService">
<port name="placeOrder"
binding="tns:placeOrderPortBinding">
<soap:address
location="https://example1.com/provider"/>
</port>
</service>
</definitions>
```

【図 2 1】

```
<RDF ...>
<rdf:Description ID="Profile">
<prf:component>
<rdf:Description ID="NetworkCharacteristics">
<prf:SecuritySupport>SSL
3.0</prf:SecuritySupport>
<prf:SupportedBearers>
<rdf:Bag>
<rdf:li>mobile Phone</rdf:li>
<rdf:li>wireless LAN</rdf:li>
</rdf:Bag>
</prf:SupportedBearers>
</rdf:Description>
</prf:component>
</rdf:Description>
</RDF>
```

【書類名】 要約書

【要約】

【課題】 ネットワーク上での認証や決済が必要となる手順において、環境やポリシーのような状況に応じてサービス要求からサービス提供までのサービス提供方法を柔軟に変更して対応し、セキュリティ強度の変更や待ち時間の短縮化を図る。

【解決手段】 サービス証明書記載内容、環境やポリシーのような状況に適応してネットワーク上のサービス手順及び／又はメッセージフォーマットを使い分ける。このサービス手順及び／又はメッセージフォーマットには送信情報のセキュリティ強度や通信路のセキュリティ強度を含み、セキュリティ強度は情報の暗号化の有無、電子署名の付加の有無により区別する。また、環境にはネットワークの伝送帯域が含まれ、その伝送帯域に応じて送信情報を使い分ける。

【選択図】 図1



特願 2002-289191

出願人履歴情報

識別番号

[392026693]

1. 変更年月日  
[変更理由]  
住 所  
氏 名

1992年 8月21日  
新規登録  
東京都港区虎ノ門二丁目10番1号  
エヌ・ティ・ティ移動通信網株式会社

2. 変更年月日  
[変更理由]

2000年 5月19日  
名称変更  
住所変更  
東京都千代田区永田町二丁目11番1号  
株式会社エヌ・ティ・ティ・ドコモ